PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-261483
(43)Date of publication of application : 22.09.2000

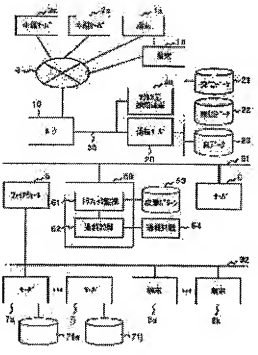
(51)Int.Cl. H04L 12/46
H04L 12/28
G06F 13/00
H04L 12/24
H04L 12/26
H04L 12/56

(21)Application number : 11-061185
(22)Date of filing : 09.03.1999

(71)Applicant : HITACHI LTD
(72)Inventor : IDEMOTO MANABU

(54) NETWORK MONITORING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a network monitoring system where an illegal access from an external network to an in-enterprise information network can be detected and a transmission source of an illegal packet can be retrieved.
SOLUTION: The network monitoring system is provided with a traffic monitoring device 50 that monitors traffic of a packet passing through a router 10 and received from an external network 3 and informs the router about identification information of an illegal packet at the time of detecting the illegal packet and with a disguised server 20 that gives a false reply to a sender of the illegal packet. The router 10 identifies the illegal packet coming from the external network and transfers the illegal packet to the disguised server based on the identification information of the illegal packet informed from the monitoring device.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－261483
（Ｐ2000－261483Ａ）
(43)公開日　平成12年９月22日（2000.9.22）

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード[*]（参考）
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ	11/00	３１０Ｃ　５Ｂ０８９
12/28		Ｇ０６Ｆ	13/00	３５１Ｚ　５Ｋ０３０
Ｇ０６Ｆ　13/00	３５１	Ｈ０４Ｌ	11/08	５Ｋ０３３
Ｈ０４Ｌ　12/24			11/20	１０２Ｚ
12/26				

審査請求　未請求　請求項の数14　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平11－61185

(22)出願日　平成11年３月９日(1999.3.9)

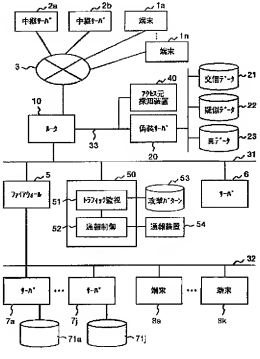
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　出本　学
東京都国分寺市東恋ヶ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　100061893
弁理士　高橋　明夫　（外１名）

Ｆターム(参考)　5B089 GA11 GA21 GA31 GB02 HA01
JB15 JB22 KA17 KB13 MC08
5K030 GA15 HA08 HC01 HC14 HD03
HD06 MA01 MB09
5K033 AA08 BA08 CC01 DA01 DA06
DB12 DB18 DB20 EA07 EC03

(54)【発明の名称】　ネットワーク監視システム

(57)【要約】
【課題】　外部ネットワークから企業内情報ネットワークへの不正アクセスを検出し、不正パケットの送信元探知を可能とするネットワーク監視システムを提供する。
【解決手段】　ルータ１０を通過する外部ネットワーク３からの流入パケットのトラフィックを監視し、不正トラフィックを検出した時、上記ルータ装置宛に不正パケットの識別情報を通知するトラフィック監視装置５０と、不正パケットの送信元に偽の応答をする偽装サーバ２０とを有し、上記ルータ１０が、監視装置から通知された上記不正パケットの識別情報に基づいて、外部ネットワークから流入する不正パケットを識別し、偽装サーバに転送する。

図　1



1

【特許請求の範囲】

【請求項１】外部ネットワークから、該外部ネットワークにルータを介して接続された内部情報ネットワークへの不正なアクセスを監視するネットワーク監視システムにおいて、

外部ネットワークから上記ルータを通過して流入するパケットのトラフィックを監視し、上記内部情報ネットワークを不正にアクセスするパケットを検出した時、上記ルータ装置宛に不正パケットの識別情報を示す制御パケットを送信するトラフィック監視装置と、

受信パケットに応答して、該パケットの送信元に、意図的な情報を含む応答パケットを送信する偽装サーバとを有し、

上記ルータが、監視装置からの上記制御パケットの受信に応答して、上記不正パケットの識別情報を記憶するための手段を備え、上記外部ネットワークから受信されたパケットの中から上記識別情報に基づいて不正パケットを識別し、上記偽装サーバに転送することを特徴とするネットワーク監視システム。

【請求項２】前記ルータが、前記外部ネットワークに接続された第１インタフェース回路と、前記内部情報ネットワークに接続された第２インタフェース回路と、前記偽装サーバに接続された第３のインタフェース回路とを有し、前記不正パケットを上記第３インタフェース回路に送出することを特徴とする請求項１に記載のネットワーク監視システム。

【請求項３】前記内部情報ネットワークが、内部情報サービス用の少なくとも１つのサーバを収容した内部セグメントと、前記ルータに接続された外部バリア・セグメントと、上記内部セグメントと上記外部バリア・セグメントとの間に接続され、上記外部バリア・セグメントから上記内部セグメントへの流入パケットを制限するためのファイアウォール装置とからなり、

前記トラフィック監視装置が、上記外部バリア・セグメントに接続され、上記外部バリア・セグメント上を流れるパケットのトラフィックを監視することを特徴とする請求項１に記載のネットワーク監視システム。

【請求項４】前記偽装サーバが、前記外部バリア・セグメントに接続され、前記ルータが、前記不正パケットの宛先アドレスを上記偽装サーバを示すアドレスに変更した後、上記外部バリア・セグメントに送出することを特徴とする請求項３に記載のネットワーク監視システム。

【請求項５】前記偽装サーバに付随して、該偽装サーバが受信する不正パケットの送信元を逆探知するための通信動作を行う送信元探知装置を備えたことを特徴とする請求項１～請求項４の何れかに記載のネットワーク監視システム。

【請求項６】外部ネットワークから、該外部ネットワークにルータを介して接続された内部情報ネットワークへの不正なアクセスを監視するネットワーク監視システムにおいて、

2

上記外部ネットワークから上記ルータを通過して流入するパケットのトラフィックを監視し、予め記憶された不正アクセスに特有の特徴をもつトラフィックを検出した時、該トラフィックに属した不正パケットの識別情報を含む制御パケットを生成して、上記ルータ装置宛に送信するトラフィック監視装置と、

受信パケットに応答して、該パケットの送信元に、意図的な情報を含む応答パケットを送信する偽装サーバとからなり、

上記ルータが、不正パケットの識別情報と出力回線との対応関係を記憶するためのフィルタリングテーブル手段と、受信パケットに含まれる宛先アドレスと出力回線との対応関係を記憶するためのルーティンテーブルと、上記監視装置から受信した制御パケットに応じて上記フィルタリングテーブルの内容を更新するための手段と、上記フィルタリングテーブルに基づいて、上記外部ネットワークから受信パケットが不正パケットか否かを判定し、不正パケットは上記偽装サーバが接続された出力回線に転送し、正常パケットは上記ルーティングテーブルに基づいてルーティング処理するための手段とを備えたことを特徴とするネットワーク監視システム。

【請求項７】前記ルータが、前記偽装サーバに専用のインタフェース回路を有し、前記各不正パケットを上記偽装サーバに専用のインタフェース回路の出力することを特徴とする請求項６に記載のネットワーク監視システム。

【請求項８】前記内部情報ネットワークが、内部情報サービス用の少なくとも１つのサーバを収容した内部セグメントと、前記ルータに接続された外部バリア・セグメントと、上記内部セグメントと上記外部バリア・セグメントとの間に接続され、上記外部バリア・セグメントから上記内部セグメントへの流入パケットを制限するためのファイアウォール装置とからなり、

前記トラフィック監視装置が、上記外部バリア・セグメントに接続され、上記外部バリア・セグメント上を流れるパケットのトラフィックを監視することを特徴とする請求項６に記載のネットワーク監視システム。

【請求項９】前記偽装サーバが、前記内部情報ネットワークの一部を構成し、前記ルータが、前記各不正パケットの宛先アドレスを上記偽装サーバ宛のアドレスに変換した後、上記内部情報ネットワークが接続されたインタフェース回路に出力することを特徴とする請求項６または請求項８に記載のネットワーク監視システム。

【請求項１０】前記偽装サーバに付随して、該偽装サーバが受信する不正パケットの送信元を逆探知するための通信動作を行う送信元探知装置を備えたことを特徴とする請求項６～請求項９の何れかに記載のネットワーク監視システム。

【請求項１１】外部ネットワークから、該外部ネットワ

ークにルータを介して接続された内部情報ネットワークへの不正なアクセスを監視するネットワーク監視システムにおいて、

上記内部情報ネットワークが、内部情報サービス用の少なくとも１つのサーバを収容した内部セグメントと、前記ルータに接続された外部バリア・セグメントと、上記内部セグメントと上記外部バリア・セグメントとの間に接続され、上記外部バリア・セグメントから上記内部セグメントへの流入パケットを制限するためのファイアウォール装置と、外部ネットワークから上記外部バリア・セグメントに流入するパケットのトラフィックを監視し、上記内部情報ネットワークを不正にアクセスするパケットを検出した時、上記ファイアウォール装置宛に不正パケットの識別情報を示す制御パケットを送信するトラフィック監視装置と、上記ファイアウォール装置から転送された受信パケットに応答して、該パケットの送信元に、意図的な情報を含む応答パケットを送信する偽装サーバとを有し、

上記ファイアウォール装置が、上記監視装置からの受信した制御パケットに基づいて、上記不正パケットの識別情報を記憶しておき、上記外部ネットワークから受信されたパケットの中から上記識別情報に基づいて不正パケットを識別し、上記偽装サーバに転送することを特徴とするネットワーク監視システム。

【請求項１２】前記偽装サーバに付随して、該偽装サーバが受信する不正パケットの送信元を逆探知するための通信動作を行う送信元探知装置を備えたことを特徴とする請求項１１に記載のネットワーク監視システム。

【請求項１３】外部ネットワークと内部ネットワークとの間に配置されたルータと、上記ルータを通過する上記外部ネットワークからの流入パケットのトラフィックを監視することによって、上記内部ネットワークを不正にアクセスする不正パケットを検出するためのトラフィック監視装置と、上記外部ネットワークと内部ネットワークとの間において上記ルータから不正パケットを受信し、該不正パケットの送信元に応答パケットを送信するサーバとを有し、

上記トラフィック監視装置が、上記内部ネットワークを不正にアクセスする不正パケットが検出された場合に、上記ルータに対して、該不正パケットのヘッダ情報で識別されるその後の特定の受信パケットを上記サーバに転送させるための制御情報を通知するための手段を有し、

上記サーバが、上記内部ネットワークに接続された他のサーバが保持するデータの一部、または上記他のサーバとは異なるデータに基いて、上記応答パケットを生成することを特徴とするネットワークシステム。

【請求項１４】前記サーバが受信する不正パケットを監視し、該不正パケットの送信元を逆探知するための手段を有することを特徴とする請求項１３に記載のネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク監視システムに関し、更に詳しくは、外部の通信ネットワークから企業内情報ネットワークへの不正アクセスに対処するための監視システムに関する。

【０００２】

【従来の技術】インターネット等の外部通信ネットワークと企業内ネットワークとを接続する場合、外部から企業内情報システムへの不正侵入の防止手段として、ファイアウォール装置が知られている。ファイアウォールは、外部ネットワークからアクセスできる外部バリア・セグメントと、企業内情報ネットワークを構成する各種のサーバおよびユーザ端末が接続される内部セグメントとの間に位置し、外部から到着する不正なパケットを識別して、内部セグメントへの侵入を阻止する。

【０００３】ファイアウォールの機能については、例えば、日経コミュニケーション、１９９６年７月１日、第６８頁～第８３頁に記載されているように、幾つかの方式が知られており、例えば、ＴＣＰ／ＩＰレイヤでアクセス制御するパケット・フィルタリング方式では、ＴＣＰ／ＩＰパケットの送信元アドレスと、宛先アドレスと、ポート番号とをチェックすることによって、パケットを通過させるか否かを判断している。上記ポート番号は、ＴＣＰ／ＩＰアプリケーション毎に予め決まった値となっており、予め登録された番号以外のポート番号をもったパケットは、ファイアウォールにおいて通過を拒否される。

【０００４】また、企業内情報システムに対する不正侵入を監視するツールとして、例えば、日経オープンシステム、１９９８年８月（No.65）第１３０頁～第１３２頁には、ネットワーク上を流れるパケットのトラフィックを監視し、予め用意されている不正アクセスに特徴的なトラフィックパターン（攻撃パターン）と比較することによって、不審なトラフィックを検出する監視ツールが記載されている。上記監視ツールによって不審なトラフィックが検知されると、例えば、アラートの表示、コネクションの切断、重要ログ情報の保存等の措置がとられる。

【０００５】

【発明が解決しようとする課題】企業内情報ネットワークへの侵入を図る不正ユーザが、外部ネットワークに接続された中継サーバを介して、企業内情報ネットワーク（以下、内部ネットワークと言う）をアクセスした場合、内部ネットワークからは、上記中継サーバが不正パケットの送信元（アクセス元）に見えるため、不正ユーザの操作する端末装置が隠蔽されてしまう。外部ネットワークから内部ネットワークへの不正侵入を検出した時点で、もし、該当コネクションを直ちに切断した場合、企業内情報の外部への漏洩やファイル情報の破壊等、そ

の後の被害を防止することができる。しかしながら、コネクションの切断によって不正パケットが途絶した状況下では、上記不正ユーザが操作する送信元端末の逆探知が困難となる。逆に、上記不正アクセスの中継点を含むパケットの侵入経路を逆探知できる迄、上記不正コネクションの切断を遅らせた場合は、外部に漏洩する情報量が増え、不正アクセスによって情報ファイルが破壊される危険性が増大するという問題がある。

【0006】重要な企業内情報の漏洩を防止し、不正アクセスの記録を残すことによって、不正端末の特定作業を支援するための従来技術の1つとして、例えば、特開平09-266475号公報では、ネットワークに接続された複数の端末装置の宛先アドレスを管理するアドレステーブルを備え、ネットワーク端末からの宛先アドレス問合せメッセージに応答して宛先アドレス通知メッセージを回答するアドレス管理サーバ、例えば、DNS(Domain Name System)や、ATM網のLECS (LAN Emulation Configuration Server)等のサーバに、問合わせメッセージの送信元を識別するための認証手段を設けておき、不正ユーザからの問合わせに対しては、上記ネットワークに接続された侵入対策用端末のアドレスを通知するようにしている。上記侵入対策用端末は、不正ユーザがアクセスしたいデータファイルは持っていないが、通信プロトコルの規定に従って不正ユーザと通信する機能と、不正ユーザからの受信パケットの内容を記録するための機能を備えており、不正ユーザからの要求に対して「該当情報なし」と回答しながら、不正ユーザとの交信期間中に受信パケットの内容を記録し、要求元アドレスの割り出しに必要な情報を収集するようになっている。

【0007】しかしながら、上記公開公報に示された従来技術は、端末からの宛先アドレスに回答するDNSやLECS等のサーバにおいて、受信メッセージの送信元アドレスから不正な問合わせを検出するものであり、宛先アドレスの問合わせを行うことなく企業内情報ネットワークに不正侵入を企てる端末ユーザに対しては有効ではない。また、上記従来技術では、侵入対策用端末が、不正ユーザからの情報要求に対して「該当情報なし」を回答するのみであるから、不正ユーザが宛先装置に不審を抱き、要求元の割り出しに必要な十分なデータを入手する前に、あるいは送信元の逆探知に成功する前に、交信が切断される可能性がある。

【0008】本発明の目的は、外部ネットワークから企業内情報ネットワークへの不正侵入を検知し、企業内の重要な情報を漏洩することなく、不正ユーザの逆探知に必要な通信保持あるいはデータ収集が可能なネットワーク監視システムおよびネットワークシステムを提供することにある。

【0009】

【課題を解決するための手段】上記課題を解決するために、本発明では、外部ネットワークから該外部ネットワークにルータを介して接続された内部情報ネットワークへの不正なアクセスを監視するネットワーク監視システムにおいて、外部ネットワークから上記ルータを通過して流入するパケットのトラフィックを監視し、上記内部情報ネットワークを不正にアクセスするパケットを検出した時、上記ルータ装置宛に不正パケットの識別情報を示す制御パケットを送信するトラフィック監視装置と、受信パケットに応答して、該パケットの送信元に意図的な情報を含む応答パケットを送信するサーバとを有し、上記ルータが、監視装置から受信した上記制御パケットに応答して、上記不正パケットの識別情報を記憶するための手段を備え、上記外部ネットワークから流入する受信パケットの中から上記識別情報に基づいて不正パケットを識別し、上記サーバに転送することを特徴とする。

【0010】尚、ここで言う意図的な情報は、例えば、擬似データファイルに予め用意された偽情報や、真の情報処理結果を改変して得られた疑似情報の他に、外部に漏洩しても問題のない真の情報をも含むものであって、監視システム側で不正アクセスが検知済みであることをユーザに悟られることなく、不正ユーザとの交信を持続するために意識的に提供される情報を意味している。本明細書では、不正パケットの送信元に対して、真のサーバに代わって、このような意図的な情報を含む応答パケットを送信するサーバを擬似サーバと言う。

【0011】本発明の1つの実施形態では、上記ルータが、外部ネットワークに接続された第1インタフェース回路と、内部情報ネットワークに接続された第2インタフェース回路と、偽装サーバに接続された第3インタフェース回路とを有し、不正パケットを上記第3インタフェース回路に送出することを特徴としている。上記第3インタフェースを偽装サーバに専用のインタフェースとすれば、ルータで受信パケットの宛先アドレスを書き替えることなく、不正パケットを偽装サーバに供給できる。

【0012】上記内部情報ネットワークは、例えば、内部情報サービス用の少なくとも1つのサーバを収容した内部セグメントと、上記ルータに接続された外部バリア・セグメントと、上記内部セグメントと上記外部バリア・セグメントとの間に接続され、外部バリア・セグメントから内部セグメントへの流入パケットを制限するためのファイアウォール装置とを備えた構成とする。内部情報ネットワークが、このようにファイアウォール装置を備えた構成となっている場合、上記外部バリア・セグメントにトラフィック監視装置を接続し、上記ルータから上記外部バリア・セグメントに出力されたパケットのトラフィックを監視させればよい。尚、本発明において、上述した偽装サーバは、必ずしもルータに直結する必要はなく、例えば、上記外部バリア・セグメントに接続してもよい。この場合、ルータにアドレス変換機能をもた

せ、不正パケットについては、宛先アドレスを上記偽装サーバ宛のアドレスに変更した後、上記外部バリア・セグメントに送出する。

【００１３】本発明の好ましい実施形態では、ネットワーク監視システムが、上記偽装サーバに付随して、該偽装サーバが受信する不正パケットの送信元を逆探知するための通信動作を行う送信元探知装置を備えることを特徴とする。本発明によれば、不正ユーザからの要求に応答して、偽装サーバが要求元に偽情報を送信するようになっているため、不正ユーザを欺き、偽装サーバと不正ユーザとの間の交信を比較的長時間にわたって継続させることが可能となる。従って、不正ユーザが偽装サーバと交信中に、上記探知装置から不正パケットの中継経路を逆方向に辿って、送信元の端末を逆探知することが可能となる。また、偽装サーバと不正ユーザとが交信中に、偽装サーバが受信した不正パケットの内容、あるいは偽装サーバから不正ユーザに送信した応答パケットの内容等、不正アクセスの証拠となるデータを保存しておくことによって、これらの証拠データを不正ユーザの追跡や新たな不正行為の予防に利用できる。上記証拠データの保存機能は、上述した偽装サーバまたは探知装置に持たせればよい。

【００１４】本発明のネットワーク監視システムにおいて、内部情報ネットワークと外部ネットワークとを接続するルータは、例えば、不正パケットの識別情報と出力回線との対応関係を記憶するためのフィルタリングテーブル手段と、受信パケットに含まれる宛先アドレスと出力回線との対応関係を記憶するためのルーティングテーブルと、上記監視装置から受信した制御パケットに応じて上記フィルタリングテーブルの内容を更新するための手段と、上記フィルタリングテーブルに基づいて、上記外部ネットワークからの受信パケットが不正パケットか否かを判定し、不正パケットは上記偽装サーバが接続された出力回線に転送し、正常パケットは上記ルーティングテーブルに基づいてルーティング処理するための手段とを備えることを特徴とする。

【００１５】偽装サーバが、内部情報ネットワークの一部を構成している場合、上記ルータで、各不正パケットの宛先アドレスを上記偽装サーバ宛のアドレスに変換した後、上記内部情報ネットワークに出力する必要がある。この場合、アドレス変換に必要な不正パケット識別情報と偽装サーバアドレスとの対応関係は、上記フィルタリングテーブル手段から得ることができる。

【００１６】本発明において、上述した偽装サーバへの不正パケットの転送機能は、上記ルータの代りに、ファイアウォール装置で行うようにしてもよい。ファイアウォールは、特定のパケットのみを内部セグメントに転送する一種のルータ機能を備えているため、トラフィック監視装置で検出した不正パケットの識別情報をファイアウォールに通知すれば、その後に到着する不正パケットをファイアウォールから偽装サーバに転送することも可能である。この場合、ファイアウォールが備えるインタフェース回路の１つに偽装サーバを接続しておけば、宛先アドレスを変換することなく、不正パケットを偽装サーバに供給できる。

【００１７】

【発明の実施の形態】以下、本発明の実施例を図面を参照して説明する。図１は、本発明によるネットワーク監視システムの１実施例を示すブロック図である。端末装置１ａ～１ｎと中継サーバ２ａ～２ｂは外部ネットワーク３に接続され、企業内情報ネットワークの外部バリア・セグメント３１が、ルータ１０を介して、上記外部ネットワーク３に結合されている。また、上記ルータ１０には、信号線３３を介して、後述する偽装サーバ２０と、不正パケットの送信元（アクセス元）探知装置４０とが接続されている。

【００１８】上記外部バリア・セグメント３１には、企業内情報ネットワークの内部セグメント（企業内ＬＡＮ）３２への不正侵入を防止するためのファイアウォール装置５と、企業内情報ネットワークへの不正アクセスを検知するための監視装置５０と、例えばメールサーバのように、外部ネットワークのサーバと通信して情報を蓄積するためのサーバ６が接続されている。また、上記内部セグメント３２には、各種の情報サービスを行うための複数のサーバ７（７ａ～７ｊ）と、企業内ユーザが操作する複数の端末装置８（８ａ～８ｋ）とが接続されている。

【００１９】外部ネットワーク３からルータ１０に到着するＩＰパケットは、例えば、図２に示すように、ＴＣＰパケット３２０とＩＰヘッダ３３０とからなる。上記ＴＣＰパケット３２０は、ユーザ情報が設定される可変長の情報部３００とＴＣＰヘッダ部３１０とからなり、ＴＣＰヘッダ部３１０は、送信元ポート番号３１１、宛先ポート番号３１２、その他のヘッダ情報を含む。また、ＩＰヘッダ３３０は、送信元ＩＰアドレス３３１、宛先ＩＰアドレス３３２、プロトコル識別子３３３、その他のヘッダ情報を含んでいる。

【００２０】図３は、ルータ１０の構成を示す。ルータ１０は、外部ネットワーク３との間でパケットを送受信するためのインタフェース回路１１Ａと、外部バリア・セグメント３１との間でパケットを送受信するためのインタフェース回路１１Ｂと、偽装サーバ２０とアクセス元探知装置４０が接続された信号線３３との間でパケットを送受信するためのインタフェース回路１１Ｃと、これらのインタフェース回路１１（１１Ａ～１１Ｃ）に内部バス３０を介して結合され、インタフェース回路間のパケット転送を制御するルーティング制御装置１２とからなる。

【００２１】上記ルーティング制御装置１２は、マイクロプロセッサによって構成され、パケットアドレスと出

力回線（インタフェース回路）との関係を定義したルーティング・テーブル１４０とフィルタリング・テーブル１５０とを記憶するためのメモリ１４と、ルーティング制御に必要な各種のプログラムを格納したプログラムメモリ１５とを備えている。

【００２２】上記プログラムメモリ１５には、後述するように、監視装置５０から受信した制御パケットに従って、上記フィルタリングテーブル１５０を更新するためのテーブル管理モジュール１１０と、上記ルーティングテーブル１４０とフィルタリングテーブル１５０とを参照して、各インタフェース１１（１１Ａ～１１Ｃ）からの受信パケットを他の何れかのインタフェースに転送するルーティングモジュール１２０とを備えている。

【００２３】ファイアウォール装置５は、通過許容パケットを識別するための定義情報を記憶したテーブルを備えており、ルータ１０によって外部バリア・セグメント３１に取り込まれた各ＩＰパケットのヘッダ情報を上記定義情報に基づいてチェックする。ファイアウォール装置５は、例えば、使用プロトコル、送信元アドレス、ユーザ等によって識別された特定のパケットについて、内部セグメント３２への通過を許容することによって、内部セグメント３２に結合されたサーバ７ａ～７ｊへの不正なアクセスを防止する。

【００２４】上記ファイアウォール装置５を潜り抜けて、企業内サーバ７ａ～７ｊを不正にアクセスしようとするユーザは、送信パケットのヘッダ情報から直接的に送信元端末が発覚するのを避けるため、１つあるいは複数の中継サーバを経由した形で、企業内情報システムのサーバ７をアクセスする場合がある。例えば、端末装置１ａのユーザが、最終的に中継サーバ２ａを経由して、不正パケットを送信した場合、パケットの送信元アドレスは、上記最終的な中継サーバ２ａのアドレスとなっている。不正ユーザは、もし、ファイアウォール５を潜り抜けるためにパケットが備えるべき正しいヘッダ情報が判らない場合、ヘッダ情報の一部、例えば、プロトコル（サービス種類）を識別するための宛先ポート番号等を順次に変更しながら、目的のサーバから何らかの応答があるまで、次々と不正パケットを送信する。

【００２５】監視装置５０は、不正アクセスを試みた場合のパケットのトラフィックに現れる幾つかの特徴的なパターン（攻撃パターン）を記憶したデータファイル５３と、外部バリア・セグメント３１に流れるパケットのトラフィックを監視し、上記データファイルに登録された不正アクセスのパターンに類似した不正トラフィックを検知するためのトラフィック監視機能５１と、不正トラフィックが検知された時、保守員に通知するために通報装置５４に警報メッセージを出力する通報制御機能５２を備えている。本発明では、不正トラフィックを検知した時、上記トラフィック監視機能５１に、通報装置５４の警報メッセージを出力すると共に、ルータ１０に対して、その後に到着する不正パケットを擬似サーバ２０宛に転送させるための制御パケットを通知させる。

【００２６】上記監視装置５０は、具体的には、外部バリア・セグメント３１との間でパケットを送受信するための通信インタフェースと、受信パケットから主要なヘッダ情報を抽出するための回路と、予め用意されたプログラムを実行するプロセッサとからなる。上述したトラフィック監視機能５１は、受信パケットから抽出されたヘッダ情報を解析し、同一送信元から送信された一連のパケットについて、ヘッダ情報の時間的変化が示す特徴パターンを抽出し、上記データファイル５３に登録してある攻撃パターンと照合するためのデータ処理プログラムによって実現される。

【００２７】図４は、不正なトラフィック、すなわち、不正パケットが検出された場合に監視装置５０からルータ１０宛に送信される制御パケット５００のフォーマットの１例を示す。上記制御パケット５００は、パケットヘッダ５１０と、情報部５２０とからなる。パケットヘッダ５１０は、図２に示したＩＰパケットのヘッダ３３０と同一のフォーマットを有し、送信元アドレス５１１として監視装置５０のアドレス、宛先アドレス５１２としてルータ１０のアドレスを含む。また、情報部５２０は、ルータ１０にパケット転送先の登録を指示するための制御命令フィールド５２１と、不正パケットの送信元ＩＰアドレスを示すフィールド５２２と、不正パケットの現在の宛先ＩＰアドレスを示すフィールド５２３と、不正パケットの転送先ＩＰアドレスを示すフィールド５２４とからなり、上記転送先フィールド５２４には偽装サーバ２０のアドレスが設定される。

【００２８】図５は、ルータ１０のルーティング・モジュール１２０が参照するルーティングテーブル１４０の構成の１例を示す。ルーティングテーブル１４０は、宛先ＩＰアドレスの特定のビット部分を抽出するためのマスクとなるビットパターンあるいは位置情報が設定されるマスク１４１と、上記マスクによって抽出された部分的な宛先ＩＰアドレスが設定される宛先ＩＰアドレス・フィールド１４２と、受信パケットの送出先となる出力回線あるいはインタフェース回路の識別子を示す出力回線フィールド１４６とを有し、この他に必要に応じて、次サーバやプロトコル情報等を示すためのフィールド１４８を含む。

【００２９】図６は、フィルタリングテーブル１５０の構成の１例を示す。フィルタリングテーブル１５０は、送信元ＩＰアドレス・フィールド１５１と、宛先ＩＰアドレス・フィールド１５２と、転送先ＩＰアドレス・フィールド１５３と、出力回線フィールド１５４とからなる。上記フィルタリングテーブル１５０は、監視装置５０から転送先登録を指令する制御パケット５００を受信した時、ルータ１０のテーブル管理モジュール１１０によって更新される。

【００３０】図６に例示したエントリＲ１００は、図４に例示した制御パケット５００の受信に応答して登録されたものであり、フィールド１５１～１５３の内容は、上記制御パケット５００の情報部にあるフィールド５２２～５２４の内容と対応している。本実施例の場合、出力回線フィールド１５４には、偽装サーバ２０が接続されたインタフェース回路１１Ｃの識別子が設定される。

【００３１】図７は、ルーチングモジュール１２０の機能を示すプログラム・フローチャートを示す。上記ルーチングモジュール１２０は、インタフェース回路１１から、制御パケット５００以外の通常のＩＰパケットを受信した時に起動され、先ず、受信パケットの送信元ＩＰアドレス３３１と宛先ＩＰアドレス３３２とに基づいて、フィルタリングテーブル１５０を検索する（ステップ１２１）。検索の結果、送信元ＩＰアドレス１５１と宛先ＩＰアドレス１５２との関係が上記受信パケットと一致するエントリまたはレコードが見つかった場合は、該当エントリの出力回線フィールド１５４が示すインタフェース回路に受信パケットを転送し（ステップ１２２～１２３）、このモジュールを終了する。本実施例の場合、フィルタリングテーブル１５０に該当エントリをもつ受信パケットは、偽装サーバ２０に転送される。

【００３２】上記受信パケットと対応するエントリがフィルタリングテーブル１５０になかった場合は、受信パケットの宛先ＩＰアドレス３３２に基づいて、ルーティングテーブル１４０を検索する（ステップ１２４）。この場合、ルーティングテーブル１４０のマスクフィールド１４１が示すマスクパターンに従って、受信パケットの宛先ＩＰアドレス３３２をマスクし、得られた部分的なアドレスビットがルーティングテーブル１４０の宛先ＩＰアドレス１４２と一致するエントリ（目的エントリ）を探す。目的エントリが見つかった場合は、該エントリの出力回線フィールド１４６が示すインタフェース回路に受信パケットを送信し（ステップ１２５～１２６）、目的エントリが見つからなければ、受信パケットを廃棄し（ステップ１２７）、このプログラムモジュールを終了する。

【００３３】図８は、偽装サーバ２０の機能を示すプログラム・フローチャートである。偽装サーバ２０は、ルータ１０からＩＰパケットを受信すると、受信パケットの情報部３００を解析し、受信パケットで使用しているアプリケーションの種類を識別する（ステップ２０１）。偽装サーバ２０には、異なる複数種類のアプリケーションソフトに対応できるように、予め複数種類の処理ルーチン２１０（２１０Ａ～２１０Ｎ）が用意してあり、受信パケットは、それぞれが使用しているコマンド体系と対応したアプリケーションの処理ルーチン２１０に渡される（ステップ２０２Ａ～２０２Ｎ）。受信パケットに対応したアプリケーションの処理ルーチンがなかった場合は、その他用の処理ルーチン２０３で受信パケットを処理する。この場合は、例えば、ユーザ要求を実行できない旨を示す応答パケットが要求元に送信される。

【００３４】上記アプリケーション別の処理ルーチン２１０は、基本的には、図９に示すように、受信パケットの情報部に含まれるコマンドを解析するステップ２１１と、ファイル名を解析して、使用ファイルを特定するステップ２１２と、コマンドを実行するステップ２１３と、コマンドの実行結果を示す応答メッセージを作成して、要求元に送信するステップ２１４と、不正ユーザとの交信内容をデータファイル２１に記録するステップ２１５からなっている。

【００３５】偽装サーバ２０は、図１に示したように、不正ユーザとの交信記録を保存するためのデータファイル２１と、不正ユーザを欺くために、ユーザからの要求に応答して偽の情報処理結果を通知するために用意された擬似データファイル２２と、擬似データがない場合に企業内情報システムのサーバ７（７ａ～７ｊ）から取り寄せた真のデータを格納するための新データファイル２３とを備えており、企業内情報システムの各サーバ７が使用しているファイル名と上記２つのデータファイル２２、２３の関係を、例えば、図１０に示すファイルテーブル２４によって管理している。尚、企業にとって外部に漏洩しても影響のない機密性の低いデータファイルについては、真のデータをそのまま擬似データとして上記擬似データファイルに格納してもよい。

【００３６】上記ファイルテーブル２４は、サーバ７を示す識別子２４１と対応して、ファイル名２４２と、ディスク装置（データファイル２２および２３）におけるファイル名２４３と、データの真偽を示す属性情報２４４との関係を示している。上述したアプリケーション別の処理ルーチン２１０におけるファイル解析ステップ２１２では、上記ファイルテーブル２４を参照することによって、各受信パケットに含まれるファイル名２４２と対応した擬似データファイル２２内の偽ファイルを特定する。また、コマンド実行ステップ２１３では、上記偽ファイルに対してコマンドを実行する。

【００３７】もし、偽ファイルが用意されていない場合は、サーバ識別子２４１が示す企業内サーバ７のデータファイル７１（７１ａ～７１ｊ）から、必要なデータをデータファイル２３に転送した後、コマンドを実行する。この場合、得られた実行結果を所定のアルゴリズムで偽の実行結果に変換してから要求元に送信することによって、機密の漏洩を防止する。尚、真のデータを使用せざるを得ないコマンドの実行は、企業内サーバ７で行うようにしてもよい。この場合、例えば、偽装サーバ２０が、送信元ＩＰアドレスを偽装サーバ２０のアドレスに一旦置換えた形で不正パケットを目的の企業内サーバ７に転送することによって、上記サーバ７が偽装サーバ２０宛に応答パケットを送信するようにしておき、上記

応答パケットが示す真のコマンド実行結果を偽装サーバ２０で偽情報に変換した後、不正ユーザに送信するようにすればよい。

【００３８】上記実施例では、企業内情報ネットワークへの不正なアクセスを監視装置５０で検知し、その後に到着する不正パケットを偽装サーバ２０に転送することによって、偽装サーバ２０から尤らしい情報、実は偽の情報を不正ユーザに応答するようにしている。上記構成によれば、不正ユーザは、アクセス先から一見、尤らしい情報を受信できるため、アクセスに成功したものと判断して、その後も新たな要求パケットを次々と送信することになる。従って、偽装サーバ２０からの応答動作によって、不正ユーザとの交信時間を引き延ばし、その間の交信記録をデータファイル２１に残すことができる。

【００３９】図１に示した構成によれば、信号線３３を介して偽装サーバ２０に転送される不正ユーザからの送信パケットは、偽装サーバに付随して上記信号線３３に結合されたアクセス元探知装置４０で受信することができる。従って、偽装サーバ２０が不正ユーザとの交信を引き延ばしている間に、探知装置４０が、不正パケットの送信元アドレスで特定される中継サーバＸに警報メッセージを送信し、中継サーバＸが、不正パケットの上流側に位置した更に他の中継サーバに警報メッセージを送信する形式で、上記不正パケットの送信元端末を逆探知することが可能となる。

【００４０】図１に示した実施例では、不正ユーザとの交信記録を偽装サーバ２０のデータファイル２１に残すようにしているが、不正ユーザと偽装サーバとの間の交信記録を探知装置４０によって記憶するようにしてもよい。この場合、探知装置自身が行う不正ユーザの逆探知プロセス、または追跡結果を上記交信記録と共に残すことができるため、不正アクセスの証拠資料として利用しやすくなる。

【００４１】また、上記実施例では、偽装サーバ２０とアクセス探知装置４０を信号線３３を介してルータ１０のインタフェース回路１１Ｃに接続した構成となっているが、上記偽装サーバ２０とアクセス探知装置４０を外部バリア・セグメント３１に接続してもよい。この場合は、図６に示したフィルタリングテーブル１５０の出力回線フィールド１５４に、上記外部バリア・セグメント３１が接続されるインタフェース回路１１Ｂの識別子を設定しておき、図７に示したルーティングモジュール１２０のフローチャートにおいて、ステップ１２３で、受信パケットの宛先ＩＰアドレスを偽装サーバのアドレスに変換した後、パケット転送するようにすればよい。偽装サーバのアドレスは、ステップ１２１でフィルタリングテーブル１５０から検索した目的エントリの転送先ＩＰアドレス・フィールド１５３から得られる。

【００４２】次に、図１１～図１４を参照して本発明の第２実施例について説明する。第２実施例では、ルーティング・テーブル１４０を参照して、受信パケットの送信元アドレスもチェックすることによって、ルータ１０に、或る程度のファイアウォール機能をもたせたことを特徴としている。

【００４３】図１１は、本実施例におけるルーティングテーブル１４０の１例を示す。ルーティングテーブル１４０の各エントリは、送信元のＩＰアドレスをマスクするためのマスクパターンを示すフィールド１４１と、上記マスクパターンでマスクされた部分的な送信元ＩＰアドレスを示すフィールド１４２と、受信パケットの入力回線（インタフェース回路）の識別子を示すフィールド１４３と、宛先ＩＰアドレスをマスクするためのマスクパターンを示すフィールド１４４と、上記マスクパターンでマスクされた部分的な宛先ＩＰアドレスを示すフィールド１４５と、受信パケットの出力回線（インタフェース回路）の識別子を示すフィールド１４６と、属性フィールド１４７と、必要に応じてプロトコル等の他の項目データが設定されるフィールド１４８とからなる。

【００４４】上記属性フィールド１４７は、そのエントリで定義された送信元と宛先との関係を満たす受信パケットについての処理区分を示しており、本実施例では、出力回線フィールド１４６で指定された出力回線への受信パケットの中継を“許可”するか、“禁止”するか、または、フィルタリングテーブル１５０が指定する出力回線に“転送”すべきかを示す区分コードが設定される。

【００４５】図１２は、上記第２実施例で使用されるフィルタリングテーブル１５０の１例を示す。本実施例では、フィルタリングテーブル１５０の各エントリは、上記ルーティングテーブルのフィールド１４１～１４５と同様の、送信元および宛先情報を示すためのフィールド１６１～１６５と、転送先のＩＰアドレスを示すフィールド１６６と、出力回線識別子を示すフィールド１６７とからなっている。上記転送先フィールド１６６には、偽装サーバ２０のＩＰアドレスが設定され、出力回線フィールド１６７には、上記偽装サーバ２０が接続されたインタフェース回路１１Ｃの識別子が設定される。

【００４６】図１３は、本実施例において、監視装置５０から図４に示す制御パケット５００を受信した場合にルータ１０が実行するテーブル管理モジュール１１０のプログラムフローチャートを示す。先ず、ルーチングテーブル１４０を検索し（ステップ１１１）、制御パケット５００の情報部５２０に含まれる送信元ＩＰアドレス５２２と宛先ＩＰアドレス５２３との関係を定義したエントリ（目的エントリ）が登録済みか否かを判定する（ステップ１１２）。もし、目的エントリが既に登録済みの場合は、属性フィールド１４７が“転送”となっているか否かを判定し（ステップ１１３）、既に“転送”となっていた場合は、このルーチンを終了する。

【００４７】目的エントリの属性フィールドが“転送”

以外の場合は、その内容を“転送”を示すコードに変更（ステップ１１４）した後、フィルタリングテーブル１５０に、上記目的エントリと対応する新たなエントリを追加登録し（ステップ１１６）、このルーチンを終了する。ルーティングテーブル１４０に目的エントリが無かった場合は、受信した制御パケット５００に従って新たなエントリを生成し、これをルーティングテーブルに追加登録（ステップ１１５）した後、ステップ１１６を実行する。例えば、図４に示した内容の制御パケット５００を受信した時点で、ルーティングテーブル１４０には、図１１に例示するように、送信元サーバＸと宛先サーバＹに関して、それぞれのセグメント間の関係を定義したエントリＲ２０１のみが登録されていた場合、これらのサーバのＩＰアドレスの関係を定義した新たなエントリＲ２０２を生成し、これをテーブルサーチにおいて上記エントリＲ２０１よりも優先する位置に登録する。

【００４８】上記新たなエントリＲ２０２の入力回線フィールド１４３には、外部ネットワークと接続されたインタフェース回路１１Ａの識別子が設定され、出力回線フィールド１４６には初期値または無効データ、属性フィールド１４７には“転送”を示すコードが設定される。また、上記新たなエントリＲ２０２の送信元ＩＰアドレスフィールド１４２および宛先１ＰアドレスフィールドＩ４５には、制御パケット５００の送信元ＩＰアドレスフィールド５２２および宛先ＩＰアドレスフィールド５２３から得られたアドレスが設定され、それぞれと対応するマスクフィールド１４１、１４４には、マスク不要を示した状態となっている。

【００４９】また、図１２に例示するように、フィルタリングテーブル１５０には、サーバＸ、ＹのＩＰアドレスと、転送先アドレス（偽装サーバ２０）と、出力回線との関係を定義した新たなレコードＲ１０２が追加される。本実施例の場合、偽装サーバ２０がルータ１０のインタフェース回路１１Ｃに接続されているため、出力回線フィールド１６７には上記インタフェース回路１１Ｃを示す識別子が設定される。

【００５０】図１４は、本実施例におけるルーチングモジュール１２０の処理動作を示すプログラムフローチャートを示す。インタフェース回路１１からパケットを受け取ると、入力回線（インタフェース回路）の識別子と、受信パケットの送信元ＩＰアドレス３３１と、宛先１ＰアドレスＩ３３２とに基づいて、ルーティングテーブル１４０を検索する（ステップ１３１）。この場合、マスクパターンが指定されたエントリでは、上記送信元ＩＰアドレス３３１と宛先ＩＰアドレス３３２をマスクパターンに従ってマスクした上で、受信パケットに該当するエントリ（目的エントリ）を検索する。

【００５１】検索の結果を判定し（ステップ１３２）、もし、目的エントリが見つからなければ無ければ、受信パケットを廃棄（ステップ１３３）して、このルーチンを終了する。目的エントリが見つかった場合、目的エントリの属性フィールドＩ４７を判定し、属性フィールドが“廃棄”を示していた場合は（ステップ１３４）、パケットを廃棄して（ステップ１３３）、このルーチンを終了する。属性フィールドが“許可”を示していた場合は（ステップ１３５）、出力回線フィールドＩ４６で指定されたインタフェース回路に受信パケットを送出し（ステップ１３６）、このルーチンを終了する。上記属性フィールドが“転送”を示していた場合は、上記ルーティングテーブルの検索と同様に、フィルタリングテーブル１５０を検索し（ステップ１３７）、検索されたエントリの出力回線フィールドＩ６７が示すインタフェース回路に受信パケットを転送（ステップ１３８）した後、このルーチンを終了する。

【００５２】尚、偽装サーバ２０とアクセス元検知装置４０を外部バリア・セグメント３１に接続した場合は、上記フィルタリングテーブル１５０の出力回線フィールドＩ６７にインタフェース回路１１Ｂの識別子を設定しておき、上記ステップ１３８で、受信パケットの宛先ＩＰアドレス３３２を転送先ＩＰアドレスフィールド５２４が示す偽装サーバ２０のアドレスに変換した後、出力回線フィールドＩ６７が示す識別子に従って、インタフェース回路１１Ｂに受信パケットを送出すればよい。

【００５３】ファイアウォール装置は、ルータに類似した受信パケット処理機能をもっているため、上述した偽装サーバ２０とアクセス元探知装置４０を図１に示すファイアウォール装置５に接続し、監視装置５０が送信した制御パケット５００をファイアウォール５で受信し、ファイアウォール５が、その後に到着する不正パケットを偽装サーバ２０に転送する構成としても良い。

【００５４】

【発明の効果】以上の説明から明らかなように、本発明では、外部ネットワークから企業内ネットワークに不正にアクセスするパケットを不正アクセス・トラフィックが示す特徴に基づいて検知し、不正パケットを偽装サーバに転送し、偽装サーバから不正ユーザに意図的な情報を応答することによって、不正ユーザと偽装サーバとの間での交信を引き延ばすようにしている。従って、本発明によれば、不正ユーザが偽装サーバと交信している間に、不正パケットの経路を逆に辿って送信元を追跡し、不正ユーザ端末を逆探知するのに必要な時間を得ることができ、不正アクセスの抑制に効果がある。

【図面の簡単な説明】

【図１】本発明のネットワーク監視システムの１実施例をブロック構成図。

【図２】上記ネットワーク監視システムで使用されるパケットフォーマットの１例を示す図。

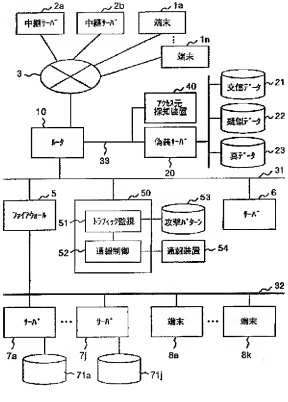
【図３】図１に示したルータ１０の詳細を示すブロック図。

【図４】図１に示した監視装置５０から送信される制御

パケットのフォーマットの１例を示す図。
【図５】ルータ１０が備えるルーティングテーブル１４０の１実施例を示す図。
【図６】ルータ１０が備えるフィルタリングテーブル１５０の１実施例を示す図。
【図７】ルータ１０が備えるルーティングモジュールの１実施例を示すプログラム･フローチャート。
【図８】図１に示した偽装サーバ２０の機能を示すプログラム・フローチャート。
【図９】図８における処理ルーチン２１０の詳細を示すフローチャート。
【図１０】上記偽装サーバ２０が備えるファイルテーブル２４の１例を示す図。
【図１１】ルータ１０が使用するルーティングテーブル１４０の他の実施例を示す図。
【図１２】ルータ１０が使用するフィルタリングテーブル１５０の他の実施例を示す図。
＊【図１３】ルータ１０が備えるテーブル管理モジュール１１０の他の実施例を示すプログラム･フローチャート。
【図１４】ルータ１０が備えるルーティングモジュール１２０の他の実施例を示すプログラム･フローチャート。
【符号の説明】
１：外部の端末装置、２：中継サーバ、３：外部ネットワーク、５：ファイアウォール装置、７：サーバ、８：内部の端末装置、１０：ルータ、１１：インタフェース回路、１２：ルーティング制御装置、２０：偽装サーバ、２２：擬似データファイル、４０：アクセス元探知装置、５０：ネットワーク監視装置、５３：攻撃パターン記憶ファイル、１１０：テーブル管理モジュール、１２０：ルーティングモジュール、１４０：ルーティングテーブル、１５０：フィルタリングテーブル、５００：制御パケット。

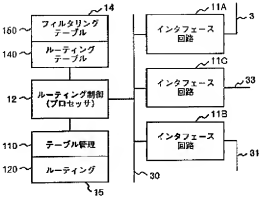
【図１】

図　1



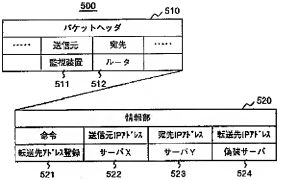
【図３】

図　3



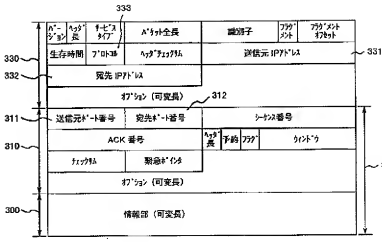
【図４】

図　4



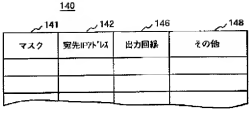
【図２】

図　２



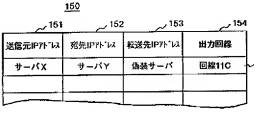
【図５】

図　５



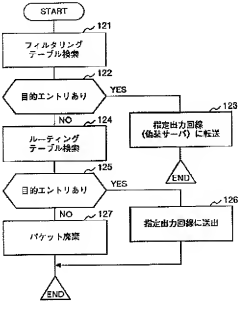
【図６】

図　６



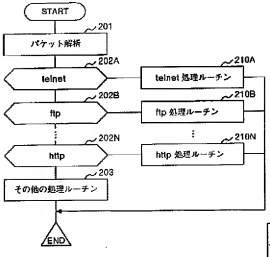
【図７】

図　７



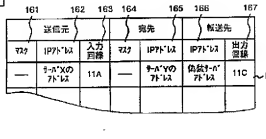
【図８】

図　８



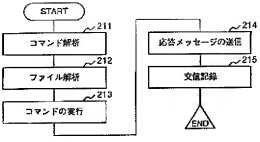
【図１２】

図　１２



【図9】

図 9



【図10】

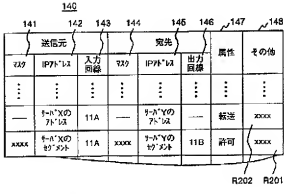
図 10

24

241 サーバ	242 ファイル名	243 ディスク位置	244 属性（真、偽）
XXXXX	/etc/password	/..../password, etc.	偽
⋮	⋮	⋮	⋮
XXXXX	/home/data	/.../131a/home/data	真
⋮	⋮	⋮	⋮

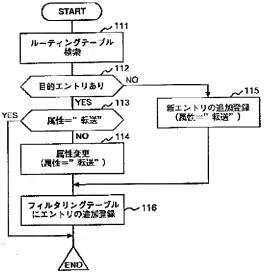
【図11】

図 11



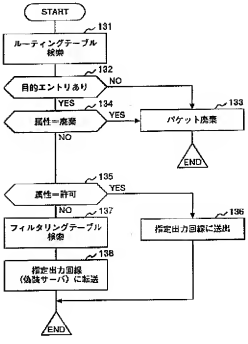
【図13】

図 13



【図１４】

図　１４



フロントページの続き

(51)Int.Cl.'	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/56			